Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ
Начальник
учебно-методического управления
Платонова Т.К.
«25» июня 2024 г.

Рабочая программа дисциплины
Основы информационной безопасности

Направление 38.03.02 "Менеджмент"
Направленность 38.03.02.11 "Финансовый менеджмент"

Для набора 2022 года

Квалификация
Бакалавр

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**5 (3.1)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	16	16	16	16
Итого ауд.	32	32	32	32
Контактная работа	32	32	32	32
Сам. работа	76	76	76	76
Итого	108	108	108	108

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 25.06.2024 г. протокол № 18.

Программу составил(и): к.т.н., доцент, Севастьянов И.Т.

Зав. кафедрой: к.э.н., доцент Радченко Ю.В.

Методический совет направления: д.э.н., профессор Суржиков М.А.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	приобретение знаний в области информационной безопасности и защиты информации по организационно-правовой защите коммерческой, служебной, профессиональной тайны, персональных данных; формирование умений и практических навыков по правовому, организационному и техническому обеспечению защиты информации при решении задач профессиональной деятельности.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ОПК-6: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

ОПК-5: Способен использовать при решении профессиональных задач современные информационные технологии и программные средства, включая управление крупными массивами данных и их интеллектуальный анализ.

В результате освоения дисциплины обучающийся должен:

Знать:

- методы и средства, обработки больших массивов данных, интеллектуального анализа и защиты информации (соотнесено с индикатором ОПК- 5.1)
- основные принципы работы систем защиты информации в соответствии с задачами профессиональной деятельности (соотнесено с индикатором ОПК-6.1)

Уметь:

- использовать инструменты для анализа больших массивов информации и мониторинга информационной безопасности в своей профессиональной деятельности (соотнесено с индикатором ОПК-5.2)
- применять средства защиты информации в рамках решения профессиональных задач (соотнесено с индикатором ОПК-6.2)

Владеть:

- применения современного компьютерного оборудования, мобильных устройств и соответствующего программного обеспечения в рамках интеллектуального анализа больших массивов данных, их безопасного использования и в соответствии со стандартами безопасности (соотнесено с индикатором ОПК-5.3)
- работы со специализированными программами для защиты и управления данными (соотнесено с индикатором ОПК-6.3)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Правовое и организационное обеспечение информационной безопасности

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетенции	Литература
1.1	Правовое обеспечение информационной безопасности в системе национальной безопасности РФ". Основные направления обеспечения информационной безопасности и защиты информации в РФ. / Лек /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.2, Л2.3, Л2.4, Л2.5
1.2	Правовое обеспечение информационной безопасности в системе национальной безопасности РФ. Базовые свойства безопасности информации. Нормативно-правовая база функционирования систем защиты информации. Правовая защита программного обеспечения авторским правом. Компьютерные преступления и особенности их расследования. / Лаб /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.2, Л2.3, Л2.4, Л2.5
1.3	Правовое обеспечение информационной безопасности в системе национальной без опасности РФ. Организация работы со сведениями, отнесенными к государственной тайне и конфиденциальной информации. / Ср /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.2, Л2.3, Л2.4, Л2.5
1.4	Выполнение заданий с использованием LibreOffice. / Ср /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

Раздел 2. Техническая защита информации

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетенции	Литература
2.1	Угрозы утечки информации по техническим каналам. Носители и формы защищаемой информации. Основные объекты защиты информации. Виды угроз безопасности информации. Технические каналы утечки информации. / Лек /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.2, Л2.3, Л2.4, Л2.5

2.2	Угрозы утечки информации по техническим каналам. Формы защищаемой информации. Объекты защиты. Физические основы возникновения ТКУИ. Классификация ТСР. / Лаб /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.2, Л2.3, Л2.4, Л2.5
2.3	Угрозы утечки информации по техническим каналам. Оценка возможностей технических средств разведки. / Ср /	5	8	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.2, Л2.3, Л2.4, Л2.5
2.4	Способы и средства технической защиты информации. Средства защиты объектов от утечки информации за счет ПЭМИ и наводок. / Ср /	5	4	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.5	Способы и средства технической защиты информации. Предотвращение утечки информации по цепям электропитания и заземления. Средства звукоизоляции и звукопоглощения акустического сигнала, оценка их эффективности. Средства поиска средств негласного съема информации. / Ср /	5	4	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.2, Л2.3, Л2.4, Л2.5
2.6	Выполнение заданий с использованием LibreOffice. / Ср /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.4, Л1.5, Л2.2, Л2.3, Л2.4, Л2.5

Раздел 3. Организация защиты информации в информационных системах

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
3.1	Организация защиты информации в информационных системах. Источники и виды угроз информации в информационных системах. Структура государственной системы технической защиты информации. Организация защиты информации. Меры защиты информации в информационных системах.Организация защиты объектов КИИ. / Лек /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.2, Л2.3, Л2.4, Л2.5
3.2	Угрозы несанкционированного доступа к информации в информационной системе. Угрозы непосредственного доступа в операционную среду информационной системы. / Ср /	5	4	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.2, Л2.3, Л2.4, Л2.5
3.3	Угрозы несанкционированного доступа к информации в информационной системе. Угрозы безопасности информации, реализуемых с использованием протоколов межсетевого взаимодействия. / Ср /	5	4	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.2, Л2.3, Л2.4, Л2.5
3.4	Угрозы несанкционированного доступа к информации в информационной системе». Угрозы программно-математических воздействий. / Ср /	5	4	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.2, Л2.3, Л2.4, Л2.5
3.5	Угрозы несанкционированного доступа к информации в информационной системе. Построение типовых моделей угроз безопасности информации, обрабатываемой в информационных системах. / Лаб /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.2, Л2.3, Л2.4, Л2.5
3.6	Требования к организации защиты информации в информационной системе. Разработка требований к мерам защиты информации, содержащейся в информационной системе. / Ср /	5	4	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.2, Л2.3, Л2.4, Л2.5
3.7	Требования к организации защиты информации в информационной системе. Обеспечение защиты информации в ходе эксплуатации информационной системы. / Ср /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.2, Л2.3, Л2.4, Л2.5
3.8	Выполнение заданий с использованием LibreOffice. / Ср /	5	2	ОПК-6, ОПК-5	Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

Раздел 4. Методы и средства криптографический защиты

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
4.1	Методы и средства криптографической защиты информации. Принципы функционирования симметричных и асимметричных криптосистем. Аутентификация с использованием открытого ключа. / Лек /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.2, Л2.3, Л2.4, Л2.5
4.2	Симметричные криптосистемы. Система шифрования Цезаря. Шифры перестановки. / Лаб /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.2, Л2.3, Л2.4, Л2.5
4.3	Симметричные криптосистемы». Шифр Гронсфельда. Шифры	5	2	ОПК-6,	Л1.1, Л1.2, Л1.3,

	многоалфавитной замены. / Ср /			ОПК-5	Л1.4, Л1.5, Л2.2, Л2.3, Л2.4, Л2.5
4.4	Асимметричные криптосистемы. Реализация двустороннего обмена ключевой информацией. Понятие и назначение центра распределения ключей. Требования Диффи и Хеллмана. / Лаб /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.2, Л2.3, Л2.4, Л2.5
4.5	Асимметричные криптосистемы. Основные математические соотношения, используемые в алгоритме RSA. Технология взлома шифра методом полного перебора. / Ср /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.2, Л2.3, Л2.4, Л2.5
4.6	Асимметричные криптосистемы. Алгоритм шифрования RSA. Процесс формирования ключевой пары получателем, шифрование и дешифрование сообщений в криптосистеме RSA. / Лаб /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.4, Л1.5, Л2.2, Л2.3, Л2.4, Л2.5
4.7	Асимметричные криптосистемы. Принципы и процедурные аспекты алгоритма электронной цифровой подписи (ЭЦП). Целостность передаваемых данных. Авторство сообщений. / Ср /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.2, Л2.3, Л2.4, Л2.5
4.8	Выполнение заданий с использованием LibreOffice. / Ср /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

Раздел 5. Лицензирование и сертификация в области защиты информации

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
5.1	Правовые основы лицензирования в области защиты информации. Структура системы государственного лицензирования. Порядок проведения лицензирования. Лицензионные требования в области защиты информации. Сертификация средств защиты информации. / Лек /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.2, Л2.3, Л2.4, Л2.5
5.2	Правовые основы лицензирования в области защиты информации». Организация лицензирования в области защиты информации. Основные лицензионные требования и условия в области защиты информации. / Ср /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.2, Л2.3, Л2.4, Л2.5
5.3	Правовые основы сертификации в РФ». Порядок проведения сертификации средств защиты информации. / Ср /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
5.4	Выполнение заданий с использованием LibreOffice. / Ср /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

Раздел 6. Основы защиты коммерческой тайны

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
6.1	Правовые основы защиты коммерческой тайны. Сущность и содержание коммерческой тайны. Правовое обеспечение защиты коммерческой тайны. Сведения, составляющие коммерческую тайну. / Лек /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
6.2	Правовые основы защиты коммерческой тайны. Порядок отнесения информации к коммерческой тайне. / Ср /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
6.3	Формирование перечня сведений, составляющих коммерческую тайну. Порядок разработки перечня сведений, составляющих коммерческую тайну. Сведения, которые не могут составлять коммерческую тайну. / Лаб /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.4, Л1.5, Л2.2, Л2.3, Л2.4, Л2.5
6.4	Правовые основы защиты коммерческой тайны». Права обладателя коммерческой тайны. / Ср /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
6.5	Правовые основы защиты конфиденциальной информации. Права и обязанности работника и работодателя по защите конфиденциальной информации. / Ср /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

6.6	Выполнение заданий с использованием LibreOffice. / Ср /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

Раздел 7. Правовые основы защиты персональных данных

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
7.1	Сущность и содержание обработки и защиты персональных данных. Права и обязанности субъекта персональных данных и оператора, обрабатывающего персональные данные. Организация защиты персональных данных в организациях, учреждениях и на предприятиях. / Лек /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
7.2	Сущность и содержание обработки и защиты персональных данных. Организация защиты персональных данных в организации. Положение об обработке и защите персональных данных в организации. / Ср /	5	4	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
7.3	Выполнение заданий с использованием LibreOffice. / Ср /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

Раздел 8. Организация защиты конфиденциальной информации на объектах информатизации

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
8.1	Организация защиты конфиденциальной информации на объектах информатизации. Сущность и содержание организационных основ защиты информации. Организационные мероприятия по обеспечению защиты информации. Организация контроля состояния защиты информации. / Лек /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
8.2	Разработка политики безопасности предприятия. / Лаб /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
8.3	Деятельность руководства и должностных лиц по проверке состояния защиты конфиденциальной информации. Организация аудита информационной безопасности. / Ср /	5	4	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
8.4	Выполнение заданий с использованием LibreOffice. / Ср /	5	2	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

Раздел 9. Промежуточная аттестация

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
9.1	/ Зачёт /	5	0	ОПК-6, ОПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущей и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература

	Авторы,	Заглавие	Издательство, год	Колич-во

	Авторы,	Заглавие	Издательство, год	Колич-во
Л1.1	Руденков Н. А., Пролетарский А. В., Смирнова Е. В., Суровов А. М.	Технологии защиты информации в компьютерных сетях: учебное пособие	Москва: Национальный Открытый Университет «ИНТУИТ», 2016	https://biblioclub.ru/index.php?page=book&id=428820 неограниченный доступ для зарегистрированных пользователей
Л1.2	Ковалев Д. В., Богданова Е. А.	Информационная безопасность: учебное пособие	Ростов-на-Дону: Южный федеральный университет, 2016	https://biblioclub.ru/index.php?page=book&id=493175 неограниченный доступ для зарегистрированных пользователей
Л1.3	Катанова, Т. Н., Галкина, Л. С., Жданов, Р. А.	Информационная безопасность: лабораторный практикум	Пермь: Пермский государственный гуманитарно-педагогический университет, 2018	https://www.iprbookshop.ru/86357.html неограниченный доступ для зарегистрированных пользователей
Л1.4	Шилов, А. К.	Управление информационной безопасностью: учебное пособие	Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2018	https://www.iprbookshop.ru/87643.html неограниченный доступ для зарегистрированных пользователей
Л1.5	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019	https://www.iprbookshop.ru/87995.html неограниченный доступ для зарегистрированных пользователей
5.2. Дополнительная литература				
	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.1		Вестник Института законодательства и правовой информации имени М.М. Сперанского: журнал	Иркутск: Институт законодательства и правовой информации, 2017	https://biblioclub.ru/index.php?page=book&id=457912 неограниченный доступ для зарегистрированных пользователей
Л2.2	Рогозин, В. Ю., Галушкин, И. Б., Новиков, В. К., Вепрев, С. Б.	Основы информационной безопасности: учебник для студентов вузов, обучающихся по направлению подготовки «правовое обеспечение национальной безопасности»	Москва: ЮНИТИ-ДАНА, 2017	https://www.iprbookshop.ru/72444.html неограниченный доступ для зарегистрированных пользователей
Л2.3	Кубашева Е. С., Малашкевич И. А., Чекулаева Е. Н.	Информатика и вычислительная техника. Информационная безопасность автоматизированных систем: учебно-методическое пособие к прохождению производственной практики: учебно-методическое пособие	Йошкар-Ола: Поволжский государственный технологический университет, 2019	https://biblioclub.ru/index.php?page=book&id=562246 неограниченный доступ для зарегистрированных пользователей
Л2.4		БИТ. Бизнес & Информационные технологии: журнал	Москва: Положевец и партнеры, 2019	https://biblioclub.ru/index.php?page=book&id=562409 неограниченный доступ для зарегистрированных пользователей
Л2.5	Суворова, Г. М.	Информационная безопасность: учебное пособие	Саратов: Вузовское образование, 2019	https://www.iprbookshop.ru/86938.html неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

Консультант+ https://www.cosultant.ru/
База данных действующих стандартов по направлению "Информационная Безопасность" https://www.gost.ru/portal/gost/home/standarts/InformationSecurity
Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России)//fstec.ru

5.4. Перечень программного обеспечения

Операционная система РЕД ОС
LibreOffice

5.5. Учебно-методические материалы для студентов с ограниченными возможностями здоровья

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:
- столы, стулья;
- персональный компьютер / ноутбук (переносной);
- проектор;
- экран / интерактивная доска.

Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными и/или свободно распространяемыми программными средствами и выходом в Интернет.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

1 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

1.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ОПК-5: Способен использовать при решении профессиональных задач современные информационные технологии и программные средства, включая управление крупными массивами данных и их интеллектуальный анализ.			
Знать: методы и средства, обработки больших массивов данных, интеллектуального анализа и защиты информации	изучает терминологию, связанную с информационной безопасностью, алгоритмы работы специализированного программного обеспечения в области ИБ, основы интеллектуального анализа больших массивов данных для подготовки к зачету, опросу	полнота и соответствие предлагаемых способов решения стандартных задач профессиональной деятельности в области информационной безопасности требованиям нормативно-правовым актов при ответе на опросе, зачете	опрос (вопросы 1-57) вопросы к зачету (вопросы 1-78)
Уметь: использовать инструменты для анализа больших массивов информации и мониторинга информационной безопасности в своей профессиональной деятельности	анализирует и оценивает уровень безопасности информационных систем, выявляет основные угрозы и уязвимости, в том числе с использованием методик интеллектуального анализа данных при выполнении практико-ориентированного и практического задания	соответствие результатов анализа текущему состоянию системы защиты информации при выполнении практико-ориентированного и практического задания	практико-ориентированные задания к зачету (задания 1-9) практическое задание (задания 1-8)
Владеть: навыками применения современного компьютерного оборудования, мобильных устройств и соответствующего программного обеспечения в рамках интеллектуального анализа больших массивов данных, их безопасного использования и в	использует методы и средства, интеллектуального анализа данных, защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России и ФСТЭК России	соответствие технологического процесса защиты информации требованиям нормативно-методических документов ФСБ России и ФСТЭК России	практико-ориентированные задания к зачету (задания 1-9) практическое задание (задания 1-8)

соответствии со стандартами безопасности			
ОПК-6: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности			
Знать: основные принципы работы систем защиты информации в соответствии с задачами профессиональной деятельности	изучает принципы конфиденциальности, целостности и доступности данных, различия между техническими и организационными мерами защиты информации для подготовки к зачету, опросу	полнота и соответствие предлагаемых способов решения стандартных задач профессиональной деятельности в области информационной безопасности требованиям нормативно-правовым актов при ответе на опросе, зачете	опрос (вопросы 1-57) вопросы к зачету (вопросы 1-78)
Уметь: применять средства защиты информации в рамках решения профессиональных задач	анализирует и выбирает средства защиты в зависимости от специфики профессиональных задач и угроз при выполнении практико-ориентированного и практического задания	соответствие результатов анализа текущему состоянию системы защиты информации при выполнении практико-ориентированного и практического задания	практико-ориентированные задания к зачету (задания 1-9) практическое задание (задания 1-8)
Владеть: навыками работы со специализированными программами для защиты и управления данными	использует инструментами для оценки уязвимостей и анализа инцидентов	качество полученных результатов, точность и полнота выявленных уязвимостей в соответствии с поставленными профессиональными задачами	практико-ориентированные задания к зачету (задания 1-9) практическое задание (задания 1-8)

1.2 Шкалы оценивания:

Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале:

50-100 баллов (зачтено)

0-49 баллов (не зачтено)

2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Вопросы к зачету

1. Информация как объект правового регулирования.
2. Структура законодательства РФ в области информационной безопасности и защиты информации.
3. Основные цели и методы обеспечения ИБ РФ. Источники и виды угроз ИБ РФ.
4. Основные направления обеспечения информационной безопасности и защиты информации в РФ.
5. Структура организационной защиты информации.
6. Виды информации, защищаемой законодательством РФ.
7. Перечень сведений конфиденциального характера.
8. Организация работы со сведениями, отнесенными к конфиденциальной информации.
9. Правовой режим защиты конфиденциальной информации.
10. Угрозы утечки информации по техническим каналам.
11. Формы защищаемой информации.
12. Основные объекты защиты информации.
13. Классификация технических каналов утечки информации.
14. Технические мероприятия по защите информации от утечки по техническим каналам.
15. Организационные мероприятия по защите информации от утечки по техническим каналам.
16. Классификация угроз безопасности информации в информационных системах.
17. Требования к организации защиты информации в информационной системе.
18. Формирование требований к защите информации в информационной системе.
19. Обеспечение защиты информации в ходе эксплуатации информационной системы.
20. Требования к мерам защиты информации, содержащейся в информационной системе.
21. Определение класса защищенности информационной системы.
22. Лицензирование в области защиты информации.
23. Структура системы государственного лицензирования.
24. Порядок проведения лицензирования.
25. Основные лицензионные требования и условия в области защиты информации.
26. Перечень видов деятельности в области защиты информации, подлежащих лицензированию.
27. Структура системы сертификации.
28. Порядок проведения сертификации средств защиты информации.
29. Сертификационные испытания средств защиты информации.
30. Порядок отнесения информации к информации, составляющей коммерческую тайну, и ее предоставление.
31. Понятие коммерческой тайны. Правовое обеспечение защиты коммерческой тайны.
32. Сведения, составляющие коммерческую тайну. Сведения, которые не могут составлять коммерческую тайну.
33. Права обладателя коммерческой тайны.
34. Организация защиты информации на предприятии.
35. Обеспечение сохранности документов, дел и изданий.
36. Обязанности лиц, допущенных к сведениям, составляющих коммерческую тайну.
37. Организация контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну.
38. Обязанности персонала организации по сохранению коммерческой тайны.

39. Политика безопасности предприятия как основа организационного управления защитой информации.
40. Права и обязанности работника и работодателя по защите конфиденциальной информации.
41. Ответственность за нарушение конфиденциальности информации.
42. Права и обязанности субъекта персональных данных и оператора, обрабатывающего персональные данные.
43. Организация защиты персональных данных в организации.
44. Планирование мероприятий по организационной защите информации на предприятии.
45. Структура и основное содержание плана мероприятий по защите конфиденциальной информации.
46. Организация аналитической работы в области защиты информации на предприятии.
47. Основные объекты и формы контроля за состоянием защиты информации.
48. Основные задачи и методы контроля.
49. Основные направления аналитической работы.
50. Организация аудита информационной безопасности предприятия.
51. Функции аналитического подразделения в области защиты информации на предприятии.
52. Основные этапы аналитической работы в области защиты информации на предприятии.
53. Содержание и основные виды аналитических отчетов.
54. Классификация методов анализа информации.
55. Компьютерные преступления в электронной коммерции.
56. Информационная безопасность в электронной коммерции.
57. Юридическая ответственность за нарушение правовых норм защиты информации.
58. Обосновать основные направления обеспечения информационной безопасности и защиты информации в РФ.
59. Выявление угроз утечки информации по каналам побочных электромагнитных излучений и наводок.
60. Выявление угроз утечки акустической (речевой) информации.
61. Выявление угроз утечки видовой информации.
62. Сформулировать технические и организационные мероприятия по защите информации от утечки по техническим каналам.
63. Выявление источников и угроз несанкционированного доступа в информационной системе.
64. Определение типов нарушителей.
65. Выявление носителей вредоносных программ.
66. Выявление уязвимостей информационной системы, системного программного обеспечения, прикладного программного обеспечения.
67. Построение типовых моделей угроз безопасности информации, обрабатываемой в информационных системах.
68. Определение класса защищенности информационной системы.
69. Сформировать требования к защите информации в информационной системе.
70. Разработка требований к мерам защиты информации, содержащейся в информационной системе.
71. Организация лицензирования в области защиты информации.
72. Организация сертификации в области защиты информации.
73. Правовое обеспечение защиты коммерческой тайны на предприятии.
74. Разработка политики безопасности предприятия.
75. Определение прав и обязанностей оператора, обрабатывающего персональные данные.
76. Определение уровня защищенности ИСПДн.
77. Определить основные объекты и формы контроля за состоянием защиты информации.
78. Сформулировать основные задачи и методы контроля.

Практико-ориентированные задания к зачету

1. Разработка концепции, программы и плана исследования.
2. Выбор метода исследования на различных этапах работы.
3. Получение первичной информации об объекте исследования с использованием инструментальных методов.
4. Обработка первичной информации об объекте исследования.
5. Разработка модели угроз нарушения информационной безопасности системы электронного документооборота
6. Разработка модели нарушителя информационной безопасности системы электронного документооборота
7. Разработка комплекта типовых эксплуатационных документов системы электронного документооборота
8. Подбор и обоснование выбора средств защиты информации и их компонентов на основании модели угроз
9. Проведение аудита защищенности системы электронного документооборота по требованиям контролирующих органов

Критерии оценивания:

Максимальное количество баллов 100. Каждое зачетное задание содержит 2 вопроса и 1 задание. Ответ на каждый вопрос оценивается отдельно, максимально 30 баллов каждый. Задание оценивается максимально 40 баллов.

Критерии оценивания ответа на отдельный вопрос:

- 25 – 30 баллов выставляется студенту, если изложенный материал фактически верен, продемонстрированы глубокие исчерпывающие знания в объеме пройденной программы в соответствии с поставленными программой курса целями и задачами обучения, изложение материала при ответе - грамотное и логически стройное;
- 20 – 24 баллов выставляется студенту, если продемонстрированы твердые и достаточно полные знания в объеме пройденной программы дисциплины в соответствии с целями обучения; материал изложен достаточно полно с отдельными логическими и стилистическими погрешностями;
- 15-19 баллов выставляется студенту, если продемонстрированы твердые знания в объеме пройденного курса в соответствие с целями обучения, ответ содержит отдельные ошибки, уверенно исправленные после дополнительных вопросов;
- 0-14 балла выставляется студенту, если ответы не связаны с вопросами, допущены грубые ошибки в ответе, продемонстрированы непонимание сущности излагаемого вопроса, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Критерии оценивания задания:

- 35-40 баллов выставляется, если задание решено полностью, в представленном решении обоснованно получены правильные ответы.
- 25-34 балла выставляется, если задание решено полностью, но при ответе допущены незначительные ошибки.
- 11-24 балла выставляется, если задание решено частично.
- 0-10 баллов выставляется, если решение неверно или отсутствует.

Итоговый результат формируется из суммы набранных баллов за выполнение зачетного задания и соответствует шкале:

- 50-100 баллов (зачтено);
- 0-49 баллов (не зачтено).

Опрос

Вопросы для опроса:

1. Информация как объект правового регулирования.
2. Структура законодательства РФ в области информационной безопасности и защиты информации.
3. Основные цели и методы обеспечения ИБ РФ. Источники и виды угроз ИБ РФ.
4. Основные направления обеспечения информационной безопасности и защиты информации в РФ.
5. Структура организационной защиты информации.
6. Виды информации, защищаемой законодательством РФ.
7. Перечень сведений конфиденциального характера.
8. Организация работы со сведениями, отнесенными к конфиденциальной информации.
9. Правовой режим защиты конфиденциальной информации.
10. Угрозы утечки информации по техническим каналам.
11. Формы защищаемой информации.
12. Основные объекты защиты информации.
13. Классификация технических каналов утечки информации.
14. Технические мероприятия по защите информации от утечки по техническим каналам.
15. Организационные мероприятия по защите информации от утечки по техническим каналам.
16. Классификации угроз безопасности информации в информационных системах.
17. Требования к организации защиты информации в информационной системе.
18. Формирование требований к защите информации в информационной системе.
19. Обеспечение защиты информации в ходе эксплуатации информационной системы.
20. Требования к мерам защиты информации, содержащейся в информационной системе.
21. Определение класса защищенности информационной системы.
22. Лицензирование в области защиты информации.
23. Структура системы государственного лицензирования.
24. Порядок проведения лицензирования.
25. Основные лицензионные требования и условия в области защиты информации.
26. Перечень видов деятельности в области защиты информации, подлежащих лицензированию.
27. Структура системы сертификации.
28. Порядок проведения сертификации средств защиты информации.
29. Сертификационные испытания средств защиты информации.
30. Порядок отнесения информации к информации, составляющей коммерческую тайну, и ее предоставление.
31. Понятие коммерческой тайны. Правовое обеспечение защиты коммерческой тайны.
32. Сведения, составляющие коммерческую тайну. Сведения, которые не могут составлять коммерческую тайну.
33. Права обладателя коммерческой тайны.
34. Организация защиты информации на предприятии.
35. Обеспечение сохранности документов, дел и изданий.
36. Обязанности лиц, допущенных к сведениям, составляющих коммерческую тайну.
37. Организация контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну.
38. Обязанности персонала организации по сохранению коммерческой тайны.
39. Политика безопасности предприятия как основа организационного управления защитой информации.

40. Права и обязанности работника и работодателя по защите конфиденциальной информации.
41. Ответственность за нарушение конфиденциальности информации.
42. Права и обязанности субъекта персональных данных и оператора, обрабатывающего персональные данные.
43. Организация защиты персональных данных в организации.
44. Планирование мероприятий по организационной защите информации на предприятии.
45. Структура и основное содержание плана мероприятий по защите конфиденциальной информации.
46. Организация аналитической работы в области защиты информации на предприятии.
47. Основные объекты и формы контроля за состоянием защиты информации.
48. Основные задачи и методы контроля.
49. Основные направления аналитической работы.
50. Организация аудита информационной безопасности предприятия.
51. Функции аналитического подразделения в области защиты информации на предприятии.
52. Основные этапы аналитической работы в области защиты информации на предприятии.
53. Содержание и основные виды аналитических отчетов.
54. Классификация методов анализа информации.
55. Компьютерные преступления в электронной коммерции.
56. Информационная безопасность в электронной коммерции.
57. Юридическая ответственность за нарушение правовых норм защиты информации.

Критерии оценивания*:*
правильный и полный ответ на 1 вопрос – 1 балл;
неправильный ответ на 1 вопрос – 0 баллов.
Максимальное количество баллов за опрос – 20 баллов.

Практические задания

Задание 1.

Работа с СПС "Консультант Плюс": Базовые свойства безопасности информации. Нормативно-правовая база функционирования систем защиты информации. Правовая защита программного обеспечения авторским правом. Компьютерные преступления и особенности их расследования.

Задание 2

Работа с СПС Консультант+, ФСТЭК России/fstec.ru, ЭБС «IPR Books» http://www.iprbookshop.ru/, Библиоклуб.ру http://biblioclub.ru/ : Формы защищаемой информации. Объекты защиты. Физические основы возникновения ТКУИ. Классификация ТСР.

Задание 3.

Работа с СПС Консультант+, ФСТЭК России/fstec.ru: Построение типовых моделей угроз безопасности информации, обрабатываемой в информационных системах.

Задание 4.

Система шифрования Цезаря. Шифры перестановки.

1. Реализовать систему шифрования Цезаря. Система шифрования Цезаря, в котором каждый символ в открытом тексте сдвигается на определенное число позиций вперед или назад. Реализовать функции шифрования и дешифрования текста с использованием системы шифрования Цезаря.
2. Реализовать шифры перестановки, в которых порядок символов в открытом тексте меняется согласно некоторой функции. Реализовать функции шифрования и дешифрования текста с использованием шифров перестановки.
3. Реализовать систему шифрования Цезаря с ключом.

4. Реализовать функции шифрования и дешифрования текста с использованием системы шифрования Цезаря с ключом.

Задание 5.

Реализация двустороннего обмена ключевой информацией. Понятие и назначение центра распределения ключей. Требования Диффи и Хеллмана.

Реализовать функции для генерации простых чисел и вычисления наибольшего общего делителя.

1. Реализовать функции для генерации ключевой пары и обмена ключевой информацией с использованием протокола Диффи-Хеллмана.
2. Реализовать тесты для функций генерации ключевой пары и обмена ключевой информацией.
3. Реализовать тесты для функций генерации ключевой пары и обмена ключевой информацией.

Задание 6.

Алгоритм шифрования RSA. Процесс формирования ключевой пары получателем, шифрование и дешифрование сообщений в криптосистеме RSA.

1. Реализовать функции для генерации простых чисел, вычисления наибольшего общего делителя, нахождения обратного элемента по модулю.
2. Реализовать функции для генерации ключевой пары и шифрования/дешифрования сообщений с использованием алгоритма RSA.
3. Реализовать тесты для функций генерации ключевой пары и шифрования/дешифрования сообщений.

Задание 7.

Формирование перечня сведений, составляющих коммерческую тайну.

1. Выберите вымышленную компанию, для которой будете формировать перечень сведений, составляющих коммерческую тайну.
2. Опишите виды сведений, которые могут составлять коммерческую тайну для выбранной компании.
3. Составьте перечень сведений, составляющих коммерческую тайну, для выбранной компании.
4. Оформите результаты в виде отчета

Задание 8.

Разработка политики безопасности предприятия.

1. Определите цели и задачи политики безопасности предприятия.
2. Опишите меры по защите информации, собственности и персонала предприятия.
3. Разработайте процедуры ответа на угрозы безопасности предприятия.
4. Оформите результаты в виде документа политики безопасности предприятия.

Критерии оценивания:

- (для каждого задания):

10 баллов. – задание выполнено верно;

9-7 баллов. – при выполнении задания были допущены неточности, не влияющие на результат;

6-3 баллов. – при выполнении задания были допущены ошибки;
2 - 1 баллов. – при выполнении задания были допущены существенные ошибки;
0 баллов. – задание не выполнено.
Максимальное количество баллов, которые могут быть получены обучающимся - 80.

3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Промежуточная аттестация проводится в форме - зачета.

Зачет проводится по расписанию промежуточной аттестации в устной форме. Количество вопросов в зачетном задании – 3 (2 теоретических, 1 практико-ориентированное задание). Результаты аттестации заносятся в ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику, должны ликвидировать задолженность в установленном порядке.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- лабораторные занятия.

В ходе лекционных занятий рассматриваются основные понятия в области информационной безопасности и защиты информации, методы обнаружения и организации противодействия атак на информационные сети, требования по защите конфиденциальной информации, даются рекомендации для самостоятельной работы и подготовки к лабораторным занятиям.

В ходе лабораторных занятий углубляются и закрепляются знания студентов по ряду рассмотренных на лекциях вопросов, развиваются навыки решения задач по защите информационных объектов.

При подготовке к лабораторным занятиям каждый студент должен:

- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;

В процессе подготовки к лабораторным занятиям студенты могут воспользоваться консультациями преподавателя.

Вопросы, не рассмотренные на лекциях и лабораторных занятиях, должны быть изучены студентами в ходе самостоятельной работы. В ходе самостоятельной работы каждый студент обязан прочитать основную и, по возможности, дополнительную литературу по изучаемой теме, дополнить конспекты лекций недостающим материалом, выписками из рекомендованных источников. Выделить непонятные термины и найти их значение в энциклопедических словарях.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.